



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

WT

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
-----------------	-------------	----------------------	---------------------

09/187,700 11/06/98 KOBAYASHI

H 3408.62676

024978
GREER, BURNS & CRAIN
300 S WACKER DR
25TH FLOOR
CHICAGO IL 60606

WM31/0925

EXAMINER

NEWTON, G
ART UNIT

PAPER NUMBER

2132
DATE MAILED:

9
09/25/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.

09/187,700

Applicant(s)

KOBAYASHI ET AL.

Examiner

Gregory A Newton

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) ____ is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☐ Claim(s) ____ is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on ____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) ____.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments with respect to claims 1-19 have been considered but are moot in view of the new ground(s) of rejection.

Amendments received and remarks have been considered. Acknowledgement of IDS JP '021 is given. Arguments concerning generation of keying data on per sector of medium basis given closer consideration.

However, Blakely et al patent reference (US 5,677,952) is found to disclose production of keying data on per sector basis. Also, concepts of *key layering*, *session keys*, and *key encrypting keys* are well known in the art.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35

U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims **1, 2, 5, 6, 8, 16-19**, rejected under 35 U.S.C. **102(b)** as being anticipated by **Blakely et al** (US 5,677,952) METHOD TO PROTECT INFORMATION ON A COMPUTER STORAGE DEVICE.

Claim **1** recites method for protecting data on storage medium. However, limitations are found within patent reference by **Blakely et al**. See e.g. ABSTRACT for generating key data, and secret (encrypted) key derived from password. Encrypting key data from password and writing encrypted key to storage medium please refer to e.g. second paragraph column 7, first sentence. Encrypting data with key data and writing encrypted data to storage medium please see e.g. ABSTRACT. Reading encrypted key from storage medium, decoding key with password, decrypting data, please refer to e.g. second paragraph column 7. Per unit storage medium basis please see e.g. ABSTRACT.

Claim **2** recites method of claim **1** with limitation of keying data generation per logic sector on medium. Please see e.g. ABSTRACT of **Blakely et al** for disclosure. Blakeley's device generates pseudorandom value (keying data) of same length as each sector used as keying data to encrypt each sector.

Claim **5** recites method of claim **1** with further limitation. Enabling of changing password and reencryption of data in **Blakely** device is disclosed top two paragraphs of column 7.

Claim **6** recites claim **1** with further limitation. Please refer to lines 57-60 column 7 of **Blakely** for disclosure of determining key data from a plurality of passwords (secrets).

Claim **8** recites storage medium protection apparatus, essentially apparatus of method claim **1**. Please refer to **Blakely et al** for such disclosures. Please refer e.g. to ABSTRACT for storage medium having plurality of unit areas. Control circuit for reading and writing data is inherently necessary. Encrypting and key from password (secret key derived from password) see e.g. first sentence of ABSTRACT. Writing secret key to disc and using secret keys to encrypt and decrypt data and write data to disc please refer e.g. to lines 15-20 column 7. Decoding and decrypting follow in logical way from encoding and encrypting. Tailoring keys to encrypt differing (i-th sector) sectors of disc is disclosed in column 5, e.g. lines 17, 64, etc.

Claim **16** recites protection of medium according to claim **1** with further limitation. Please refer to **Blakely et al**, beginning top of column 9 and subsequent paragraphs for enabling disclosures of writing secret keying data for all sectors of medium at initialization of medium.

Claim **17** recites data protection method of claim **16** with further limitations. Please refer to **Blakely et al** for disclosure. Reading of secret encryption key from disc please refer to e.g. lines 18-19 column 7. Enabling for decoding encrypted keying data with password is disclosed lines 17-18 column 7. Encrypting data with decoded key disclosed line 19 column 7.

Claim **18** recites encoding method for protecting data on storage medium.

Please refer to **Blakely et al** for such disclosures. Generation of different keying data for each area of medium please refer e.g. to ABSTRACT. Encrypting keying data by password disclosed e.g. second and third lines of ABSTRACT (deriving secret key from password). Writing secret keying data to disc see lines 15-16 column 7. Encrypting and writing encrypted data to medium using keying data see lines 17-19 column 7.

Claim **19** recites decoding method of storage medium. Please refer to **Blakely et al** for such disclosures. Forming different keying data for different sectors of medium please refer to ABSTRACT or column 5 starting line 10 for enabling disclosures of forming different keying data for each sector (i-th sector). Reading such keying data from disc please refer to e.g. line 18 column 7. Decoding such keying data using password see lines 17-19 column 7. Decoding data from medium with decoded keying data please refer e.g. to line 19 column 7.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

4. Claims **3, 4, 7, 15**, rejected under 35 U.S.C. 103(a) as being unpatentable over Blakely et al (US 5,677,952).

Claims **3** recites method of claim **1** with further limitations. Examiner takes official notice that capability is within **Blakely** system for generation of keying data as different keying data for each writing to storage. Please see e.g. paragraph lines 40-60 column 5 for different possible embodiments of Blakely device. Disclosed there are different embodiment scenarios for generation of keying data (lines 43-50), and suggesting ways to tailor key generation in reaction to different needs. Blakely device has ability to change key data by combining password with other parameters (paragraph line 40 column 5). Same device has ability to change keying data for changing password for certain user. Refer to second paragraph column 7 for disclosures of user changing password data and other parameters to alter keying data. Therefore, device has ability to change keying data for different writings.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to enable explicitly different keying data for different

writings to disk. One of ordinary skill in the art would have been motivated to do this by referring to disclosures of Blakely concerned with enabling different embodiments of storage writing device, and for maximum protection of data, which is the purpose of Blakely device. Such keying techniques are referred to in the art as belonging to class known as session keys.

Claim 4 recites method of claim 1 with further limitation. However, generating random key data is disclosed e.g. within ABSTRACT of **Blakely** reference. See e.g. lines 35-40 for embodiment references enabling combination of pieces of random numbers. Also see e.g. line 12 for reference to fitting random data to length using pieces.

Claim 7 is method dependent on claim 1 with further limitations. Encryption of one password (secret) with another is well known in the art (key encrypting keys, key layering, etc) and is referred to as two secrets being utilized together by different means, as is disclosed lines 57-60 column 7 of Blakely et al. One of ordinary skill in the art would have been motivated to employ key layering as a way to use two secret passwords, as referred to by Blakely et al lines 57-60 column 7, for additional security, disclosed as motivation e.g. line 52 column 7.

Claim 15 recites storage medium protection. Plurality of key data refer e.g. to line 57 column 7 of **Blakely** et al. Different password (secret) for each area (sector) of medium is disclosed e.g. in ABSTRACT and is enabled beginning in column 5 as disclosing enablement of keying data for each sector of medium (i-th sector). See also first paragraph column 8 for enabling separate keying data per i-th sector. Requiring

user to remember or enter a different password for each sector of disc would be asking too much of user, and so it is taken that password for each sector is a secret keying data for each sector generated by device, which is enabled beginning in column 5 e.g. line 19.

5. Claims **9-14** are apparatus claims in accordance with methods of claims **2-7**, and are rejected in view of same prior art of record and in accordance with same rationale.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2132

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gregory A Newton whose telephone number is 703-305-1373. The examiner can normally be reached on 9-6 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert DeCady can be reached on 703-305-9595. The fax phone numbers for the organization where this application or proceeding is assigned are 703-305-0040 for regular communications and 703-305-0040 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

gn

gn
September 9, 2001


ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100